УДК 621.383

А. М. ТИМОФЕЕВ, КАНД. ТЕХН. НАУК, ДОЦЕНТ

ВЛИЯНИЕ ВРЕМЕНИ ОДНОФОТОННОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ НА ДОСТОВЕРНОСТЬ ЕЕ ПРИЕМА В КВАНТОВО-КРИПТОГРАФИЧЕСКОМ КАНАЛЕ СВЯЗИ

Белорусский государственный университет информатики и радиоэлектроники

Получено выражение для оценки достоверности информации при ее передаче по квантово-криптографическому каналу связи, содержащему счетчик фотонов с мертвым временем. По результатам математического моделирования установлены зависимости достоверности принятых данных от среднего времени однофотонной передачи информации. Выполненные исследования показали, что с ростом среднего времени однофотонной передачи информации эти зависимости растут, достигая насыщения. Причем прочих равных параметрах с ростом средней длительности мертвого времени продлевающегося типа насыщение происходит при больших значениях среднего времени однофотонной передачи информации.

Ключевые слова. *Счетчик фотонов, мертвое время, квантово-криптографический канал связи.*

Введение

При создании современных систем связи стремятся повысить надежность их функционирования [1]. Это особенно важно, когда системы связи предназначены для передачи конфиденциальных данных. Так, например, в системах квантово-криптографической связи достаточно часто в качестве приемных модулей используют счетчики фотонов [2]. Обусловлено это тем, что в таких системах передача информации выполняется маломощными оптическими импульсами со средним числом фотонов не более десяти на каждый передаваемый бит (или символ). Счетчики фотонов характеризуются достаточно высокой чувствительностью [3–5], что позволяет с высокой достоверностью регистрировать предельно слабое оптическое излучение.

Под достоверностью будем понимать вероятность того, что принятые данные соответствуют переданным.

Известные методы оценки достоверности принятых данных [1] не учитывают наличие мертвого времени счетчика фотонов. В течение этого времени счетчик фотонов не чувствителен к падающему на него оптическому излучению [3, 5], что приводит к ошибкам при передаче данных и к потерям передаваемой информации.

Поскольку до настоящего времени оценка влияния мертвого времени счетчика фотонов на достоверность принятых данных квантово-криптографических каналов связи не выполнялась, то это являлось целью данной работы.

Объектом исследования являлся асинхронный квантово-криптографический канал связи, в котором в качестве приемного модуля использовался счетчик фотонов с мертвым временем продлевающегося типа. Мертвым временем продлевающегося типа характеризуются счетчики фотонов на базе лавинных фотоприемников, включенные по схеме пассивного гашения лавины [2, 3].

Предметом исследования является установление влияния времени однофотонной передачи информации на достоверность ее приема.

Выражение для оценки достоверности принятых данных

В начале получим выражение для оценки достоверности принятых данных. Дальнейшие рассуждения будут основаны на том, что канал связи построен на базе приемо-передающего оборудования [4], в котором данные передаются двоичными символами («0» и «1») в течение длительности времени τ_b. Для передачи символов «0» и «1» используются оптические сигналы мощностью W_1 и W_2 соответственно

($W_1 < W_2$), содержащие не более десяти фотонов на каждый бит (символ). Причем трансляция этих сигналов в канал связи осуществляется в течение длительности времени однофотонной передачи $\Delta t = \tau_b /2$. Следовательно, в течение времени $t_з = \tau_b /2$ данные в канал связи не передаются, т. е. между каждой парой символов находится так называемый «защитный» временной интервал. Поскольку символы «0» и «1» передаются импульсами различной мощности, то на выходе счетчика фотонов за время Δt формируется различное количество электрических импульсов, которое будет прямо пропорционально мощности оптического излучения [4]. Всеми потерями информации, за исключением потерь в счетчике фотонов, пренебрегаем.

Исходя из определения, выражения для оценки достоверностей принятых символов «0» символов «1» запишутся соответственно как:

$$D_0 = \frac{P(0/0)}{P(0/0)+P(0/1)}$$

и

$$D_1 = \frac{P(1/1)}{P(1/1)+P(1/0)}, \qquad (1)$$

где $P(0/0)$ и $P(1/1)$ – вероятности регистрации на выходе канала связи символов «0» и символов «1» при наличии на входе канала связи символов «0» и «1» соответственно, $P(0/1)$ и $P(1/0)$ – вероятности регистрации на выходе канала связи символов «0» и символов «1» при наличии на входе канала связи символов «1» и «0» соответственно.

Предположим, что на выходе канала зарегистрирована случайная двоичная последовательность, для которой вероятность появления символов «0» $P'_s(0)$ равна вероятности появления символов «1» $P'_s(1)$. Тогда достоверность принятых данных равна:

$$D = 0,5(D_0 + D_1) = 0,5\left(\frac{P(0/0)}{P(0/0)+P(0/1)} + \frac{P(1/1)}{P(1/1)+P(1/0)}\right). \qquad (2)$$

Переходные вероятности $P(0/0)$, $P(0/1)$, $P(1/1)$ и $P(1/0)$, входящие в выражение (2), для рассматриваемого канала связи получены в работе [6] на основании статистических распределений числа импульсов на выходе счетчика фотонов:

$$P(0/0) = \sum_{N=N_1}^{N_2} \frac{\left[(n_t + n_{s0})(\Delta t - \tau_d)\right]^N \exp\left[-(n_t + n_{s0})(\Delta t - \tau_d)\right]}{N!}, \qquad (3)$$

$$P(0/1) = \sum_{N=N_1}^{N_2} \frac{\left[(n_t + n_{s1})(\Delta t - \tau_d)\right]^N \exp\left[-(n_t + n_{s1})(\Delta t - \tau_d)\right]}{N!}, \qquad (4)$$

$$P(1/1) = 1 - \sum_{N=0}^{N_2} \frac{\left[(n_t + n_{s1})(\Delta t - \tau_d)\right]^N \exp\left[-(n_t + n_{s1})(\Delta t - \tau_d)\right]}{N!}, \qquad (5)$$

$$P(1/0) = 1 - \sum_{N=0}^{N_2} \frac{\left[(n_t + n_{s0})(\Delta t - \tau_d)\right]^N \exp\left[-(n_t + n_{s0})(\Delta t - \tau_d)\right]}{N!}, \qquad (6)$$

где N_1 и N_2 – нижний и верхний пороговые уровни регистрации соответственно, n_t – средняя скорость счета темновых импульсов на выходе счетчика фотонов, n_{s0} и n_{s1} – средние скорости счета сигнальных импульсов на выходе счетчика фотонов при передаче символов «0» и «1» соответственно, τ_d – средняя длительность мертвого времени продлевающегося типа.

Нижний и верхний пороговые уровни регистрации – это соответственно наименьшее и наибольшее число зарегистрированных на выходе счетчика фотонов импульсов, при котором делается вывод, что передан символ «0». При превышении зарегистрированных импульсов числа N_2 делается вывод, что передан символ «1», а при регистрации импульсов в количестве, меньшем, чем N_1, принимается решение, что символ отсутствует [4, 6].

Отметим, что для оценки мертвого времени продлевающегося типа используют среднее значение, т.к. его длительность зависит от интенсивности оптического излучения [3].

Темновые и сигнальные импульсы – это импульсы, которые появляются на выходе счетчика фотонов соответственно в отсутствии оптического сигнала и в результате воздействия фотонов регистрируемого излучения [2, 3].

Таким образом, рассчитать достоверность принятых данных можно путем подстановки в формулу (2) соответствующих выражений (3)–(6) при заданных пороговых уровнях регистрации N_1 и N_2, средних скоростях счета импульсов n_t, n_{s0} и n_{s1} и длительностях времени τ_d, Δt и τ_b.

Результаты математического моделирования и их обсуждение

Вычисление достоверности принятых данных выполнялось для каналов связи, содержащих в качестве приемного модуля счетчик фотонов с мертвым временем продлевающегося типа при различных значениях τ_d, n_{s0}, n_{s1} и Δt.

На рис. 1 представлены зависимости достоверности принятых данных от среднего времени однофотонной передачи информации для различной средней длительности мертвого времени продлевающегося типа.

При построении зависимостей $D(\Delta t)$ средние скорости счета сигнальных импульсов n_{s0} и n_{s1} и диапазоны значений Δt выбирались по методике, описанной в работе [6], с учетом того, что τ_d не может превышать Δt, которое, в свою очередь, должно быть меньше средней длительности передачи одного бита (символа) τ_b на величину защитного временного интервала. В противном случае использование счетчиков фотонов для регистрации данных становится невозможным [4, 6].

Расчет зависимостей, показанных на рис. 1, проводился для одинаковых значений нижнего и верхнего пороговых уровней регистрации $N_1 = 1$ и $N_2 = 7$, средней скорости счета темновых импульсов $n_t = 10^3$ с$^{-1}$ и средней длительности передачи одного бита (символа) $\tau_b = 100$ мкс. Необходимо отметить, что пороговые уровни регистрации можно выбирать и другими, отличными от 1 и 7, но при сравнении зависимостей $D(\Delta t)$ для различных средних длительностей мертвого времени пороговые уровни регистрации N_1 и N_2 следует фиксировать постоянными, как и среднее значение скорости счета темновых импульсов n_t и среднее время передачи одного бита (символа) τ_b.

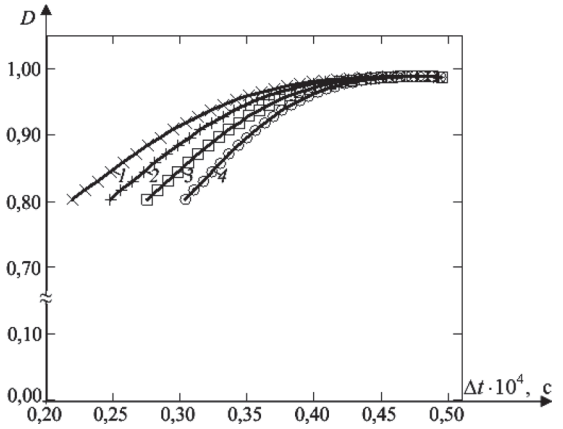

Рис. 1. Зависимость достоверности принятых данных от времени однофотонной передачи: $N_1 = 1$, $N_2 = 7$, $n_t = 10^3$ с$^{-1}$, $\tau_b = 100$ мкс; средняя длительность мертвого времени: *1* – × $\tau_d = 0$; *2* – + $\tau_d = 5$ мкс; *3* – □ $\tau_d = 10$ мкс; *4* – ○ $\tau_d = 15$ мкс

Отметим, что при других значениях N_1 и N_2, отношениях $\tau_d/\Delta t$, n_t/n_{s0} и n_t/n_{s1} и выполнении указанных выше ограничений проявление эффекта мертвого времени продлевающегося типа для рассматриваемого канала связи аналогично представленному на рис. 1.

Из полученных результатов видно, что с увеличением среднего времени однофотонной передачи информации Δt зависимости $D(\Delta t)$ растут, достигая насыщения, что имеет место для всех исследуемых значений τ_d (см. рис. 1). При прочих равных параметрах с ростом средней длительности мертвого времени продлевающегося типа τ_d это насыщение происходит при больших значениях Δt: при $\Delta t \geq 44{,}6$ мкс для $\tau_d = 0$; при $\Delta t \geq 45{,}1$ мкс для $\tau_d = 5$ мкс; при $\Delta t \geq 45{,}8$ мкс для $\tau_d = 10$ мкс; при $\Delta t \geq 46{,}3$ мкс для $\tau_d = 15$ мкс. При этом увеличение τ_d при прочих равных параметрах приводит к уменьшению достоверности принятых данных. Так, например, при $\Delta t = 42$ мкс достоверность принятых данных равна $98{,}46 \cdot 10^{-2}$ для $\tau_d = 0$; $98{,}30 \cdot 10^{-2}$ для $\tau_d = 5$ мкс; $98{,}02 \cdot 10^{-2}$ для $\tau_d = 10$ мкс; $97{,}59 \cdot 10^{-2}$ для $\tau_d = 15$ мкс. Указанные особенности поведения зависимостей $D(\Delta t)$ объясняются характером изменения переходных вероятностей $P(0/0)$, $P(0/1)$, $P(1/1)$ и $P(1/0)$ с увеличением среднего времени однофотонной передачи информации Δt, что иллюстрируется рис. 2.

С увеличением среднего времени однофотонной передачи информации Δt переходные вероятности $P(0/0)$, $P(1/0)$ и $P(1/1)$ растут, а переходная вероятность $P(0/1)$ уменьшается. Это наблюдается как при наличии мертвого

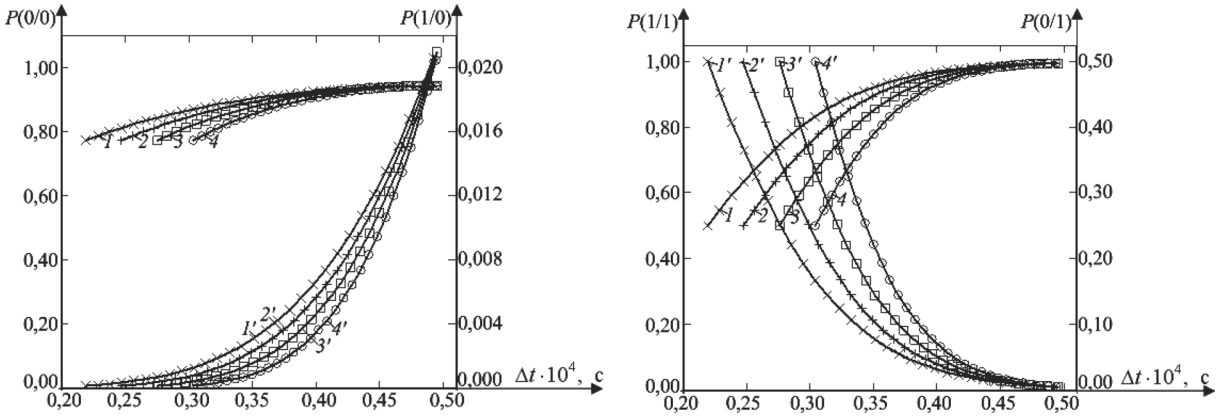

Рис. 2. Зависимости переходных вероятностей $P(0/0)$, *а*, *1–4*, $P(1/0)$, *а*, *1'–4'*, $P(1/1)$, *б*, *1–4*, $P(0/1)$, *б*, *1'–4'*, от времени однофотонной передачи: $N_1 = 1$, $N_2 = 7$, $n_t = 10^3$ с$^{-1}$, $\tau_b = 100$ мкс; средняя длительность мертвого времени: *1* и *1'*– × $\tau_d = 0$; *2* и *2'* – + $\tau_d = 5$ мкс; *3* и *3'*– □ $\tau_d = 10$ мкс; *4* и *4'*– ○ $\tau_d = 15$ мкс

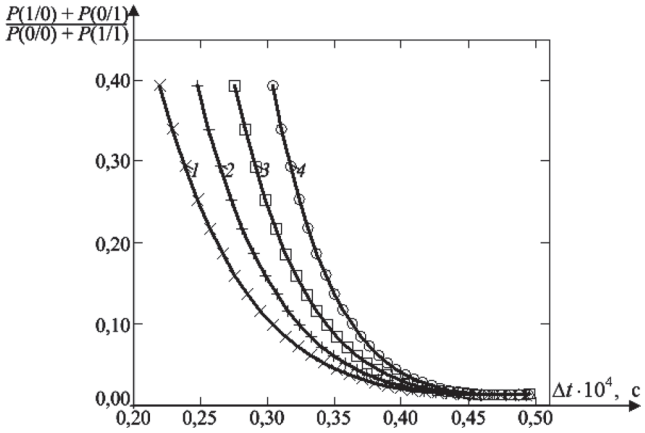

Рис. 3. Зависимость отношения $[P(1/0) + P(0/1)] / [P(0/0) + P(1/1)]$ от времени однофотонной передачи: $N_1 = 1$, $N_2 = 7$, $n_t = 10^3$ с$^{-1}$, $\tau_b = 100$ мкс; средняя длительность мертвого времени: *1* – × $\tau_d = 0$; *2* – + $\tau_d = 5$ мкс; *3* – □ $\tau_d = 10$ мкс; *4* – ○ $\tau_d = 15$ мкс

времени продлевающегося типа (см. рис. 2, кривые *2–4* и *2'–4'*), так и при его отсутствии (см. рис. 2, кривые *1* и *1'*) и объясняется смещением статистических распределений смеси числа темновых и сигнальных импульсов $P_{st0}(N)$ и $P_{st1}(N)$ при передаче символов «0» и «1» соответственно с изменением Δt и τ_d, что достаточно подробно поясняется в работе [6]. Следует также отметить, что при прочих равных параметрах приема информации в результате такого смещения с ростом τ_d переходные вероятности $P(0/0)$, $P(1/0)$ и $P(1/1)$ уменьшаются, а переходная вероятность $P(0/1)$ – растет. Так, например, при $\Delta t = 45$ мкс переходные вероятности $P(0/0)$, $P(1/0)$, $P(1/1)$ и $P(0/1)$ равны соответственно $93{,}94 \cdot 10^{-2}$, $1{,}28 \cdot 10^{-2}$, $98{,}87 \cdot 10^{-2}$ и $1{,}13 \cdot 10^{-2}$ для $\tau_d = 0$; $93{,}84 \cdot 10^{-2}$, $1{,}20 \cdot 10^{-2}$, $98{,}73 \cdot 10^{-2}$ и $1{,}27 \cdot 10^{-2}$ для $\tau_d = 5$ мкс; $93{,}70 \cdot 10^{-2}$, $1{,}10 \cdot 10^{-2}$, $98{,}51 \cdot 10^{-2}$ и $1{,}49 \cdot 10^{-2}$ для $\tau_d = 10$ мкс; $93{,}50 \cdot 10^{-2}$, $0{,}99 \cdot 10^{-2}$, $98{,}23 \cdot 10^{-2}$ и $1{,}77 \cdot 10^{-2}$ для $\tau_d = 15$ мкс (см. рис. 2). Отметим также, что для всех исследуемых диапазонов Δt наибольшее значение $P(1/0)$ не превышает наименьшей величины $P(0/0)$.

Указанные особенности изменения переходных вероятностей $P(0/0)$, $P(1/0)$, $P(1/1)$ и $P(0/1)$ с ростом Δt, в свою очередь, приводят к росту зависимостей $D(\Delta t)$ вплоть до их насыщения за счет того, что отношение $[P(1/0) + P(0/1)] / [P(0/0) + P(1/1)]$ с ростом Δt уменьшается, тоже переходя в насыщение, как показано на рис. 3.

Также из рис. 3 видно, что при прочих равных параметрах увеличение τ_d приводит к росту отношения $[P(1/0) + P(0/1)] / [P(0/0) + P(1/1)]$. Так, например, при $\Delta t = 34$ мкс это отношение равно $5{,}26 \cdot 10^{-2}$ для $\tau_d = 0$; $7{,}16 \cdot 10^{-2}$ для $\tau_d = 5$ мкс; $10{,}58 \cdot 10^{-2}$ для $\tau_d = 10$ мкс; $16{,}99 \cdot 10^{-2}$ для $\tau_d = 15$ мкс. Следовательно, при прочих равных параметрах с ростом τ_d до-

стоверность принятых данных уменьшается (см. рис. 1).

Заключение

Получено выражение для расчета достоверности данных, принятых по асинхронному квантово-криптографическому каналу связи, в котором в качестве приемного модуля используется счетчик фотонов с мертвым временем продлевающегося типа.

Установлены зависимости достоверности принятых данных D от среднего времени однофотонной передачи информации Δt с учетом средней длительности мертвого времени продлевающегося типа τ_d. Выполненные исследования показали, что с ростом среднего времени однофотонной передачи информации зависимости $D(\Delta t)$ растут, достигая насыщения. Причем прочих равных параметрах с ростом средней длительности мертвого времени продлевающегося типа τ_d это насыщение происходит при больших значениях Δt: при $\Delta t \geq 44{,}6$ мкс для $\tau_d = 0$; при $\Delta t \geq 45{,}1$ мкс для $\tau_d = 5$ мкс; при $\Delta t \geq 45{,}8$ мкс для $\tau_d = 10$ мкс; при $\Delta t \geq 46{,}3$ мкс для $\tau_d = 15$ мкс.

ЛИТЕРАТУРА

1. **Дмитриев, С. А.** Волоконно-оптическая техника: современное состояние и перспективы / С. А. Дмитриев, Н. Н. Слепов. – М.: ООО ВОТ, 2005. – 576 с.

2. **Килин, С. Я.** Квантовая криптография: идеи и практика / С. Я. Килин; под ред. С. Я. Килин, Д. Б. Хорошко, А. П. Низовцев. – Минск: Белорус. наука, 2007. – 391 с.

3. **Гулаков, И. Р.** Фотоприемники квантовых систем: монография / И. Р. Гулаков, А. О. Зеневич. – Минск: УО ВГКС, 2012. – 276 с.

4. **Тимофеев, А. М.** Устройство для передачи и приема двоичных данных по волоконно-оптическому каналу связи / А. М. Тимофеев // Приборы и методы измерений. – 2018. – т. 9. – № 1. – С. 17–27.

5. **Reduced** deadtime and higher rate photon-counting detection using a multiplexed detector array / S. A. Castelletto [et al.] // Journal of Modern Optics – 2007. – Vol. 54. – P. 337–352

6. **Тимофеев, А. М.** Энтропия потерь однофотонного асинхронного волоконно-оптического канала связи с приемником на основе счетчика фотонов с продлевающимся мертвым временем / А. М. Тимофеев // Актуальные проблемы науки XXI века. – 2018. – вып. 7. – С. 5–10.

REFERENCES

1. **Dmitriev S. A.** [Fiber-optic technology: current status and prospects]. Volokonno-opticheskaya tehnika: sovremennoe sostoyanie i perspektivyi. – Moscow: LLC FOT, 2005, 576 p. (in Russian).

2. **Kilin S. Ya.** [Quantum cryptography: ideas and practices]. Kvantovaya kriptografiya: idei i praktika. – Minsk: Belarus. Sci, 2007, 391 p. (in Russian).

3. **Gulakov I. R., Zenevich A. O.** [Photodetectors of quantum systems: monograph]. Fotopriemniki kvantovyih sistem: monografiya. – Minsk: EI HSCC, 2012, 276 p. (in Russian).

4. **Timofeev A. M.** [Device for binary data transmitting and receiving over a fiber-optic communication channel]. Priboryi i metodyi izmereniy [Devices and methods of measurements], 2018. – Vol. 9. – № 1, pp. 17–27 (in Russian).

5. **Castelletto S. A., Degiovanni I. P., Schettini V., Migdall A. L.** Reduced deadtime and higher rate photon-counting detection using a multiplexed detector array. Journal of Modern Optics, 2007, vol. 54, pp. 337–352.

6. **Timofeev A. M.** [Entropy of losses of a single-photon asynchronous fiber-optic communication channel with a receiver based on a photon counter with prolonged dead time]. Aktualnyie problemyi nauki XXI veka [Current issues of science in the 21st century], 2018, – Vol. 7, pp. 5–10 (in Russian).

Поступила *23.01.2019* | *После доработки* *20.03.2019* | *Принята к печати* *25.03.2019*

TIMOFEEV A. M.

THE INFLUENCE OF THE TIME OF SINGLE PHOTON TRANSMISSION OF INFORMATION ON THE RELIABILITY OF ITS RECEPTION IN A QUANTUM CRYPTOGRAPHIC COMMUNICATION CHANNEL

Expression for estimating the reliability of information during its transmission through quantum-cryptographic communication channel that contains a dead time photon counter has been obtained in this research. According to the results of mathematical modeling, the dependence of the reliability of the received data on the average time of single photon transmission of information was established. Studies have shown that with an increase in the average time of single photon transmission of information, these dependences grow, reaching saturation. Moreover, with equal parameters with an increase in the average duration of the dead time of a prolonging type, saturation occurs at large values of the average time of a single photon transmission of information.

Keywords. *Photon counter, dead time, quantum cryptographic communication channel.*

Тимофеев Александр Михайлович, кандидат технических наук, доцент, доцент кафедры защиты информации Белорусского государственного университета информатики и радиоэлектроники, г. Минск, Республика Беларусь.

E-mail tamvks@mail.ru